



# Big Tech's Free Online Services Aren't Costing Consumers Their Privacy

HADI HOUALLA | SEPTEMBER 2023

---

There is no evidence that breaking up big online platforms will improve digital privacy, but there is overwhelming evidence that breaking up these services or restricting them from collecting user data will harm consumers and workers.

---

## KEY TAKEAWAYS

- Data is what economists call a “nonrivalrous good,” meaning multiple parties can use data without depleting the data available to others.
- As such, when consumers share their data with companies to access free online services, they experience no loss, unlike when they pay for services with money.
- Targeted advertising based on user data enables companies to provide highly valuable services to consumers for free, supports a thriving R&D ecosystem, and creates a high-value-added tech sector that benefits American workers.
- Targeted ads do not harm consumers. Restricting this practice would lower ad effectiveness at a cost of \$33 billion a year to the U.S. economy.
- Alternative online services that do not use targeted advertising, such as DuckDuckGo, already exist, but are unpopular with consumers, so antitrust interventions to deconcentrate tech are unlikely to change consumer preferences.
- Banning targeted ads would force companies to monetize their services with subscription fees against the wishes of consumers and at the expense of low-income consumers.

**CONTENTS**

Key Takeaways..... 1
Introduction..... 2
Data Is Not Like Money..... 3
Use of Data to Target Ads Is Not a Consumer Harm ..... 3
Consumers Already Have Privacy-Protective Options ..... 5
Consumers Don’t Want to Pay for Online Services that Are Already Free..... 6
Conclusion ..... 6
Endnotes..... 7

**INTRODUCTION**

U.S. antitrust doctrine has long focused on the consumer welfare standard, particularly the effect of competition on prices. This poses a challenge for anti-“Big Tech” activists (neo-Brandeisians) because many digital services—search, social media, and so forth—are free. So where is the consumer harm from more concentrated markets? There is none.

Without a theory of harm, a core justification for aggressive antitrust action is lacking. Therefore, neo-Brandeisians have concocted a new harm: People are not only paying with their data, but they are also paying too much. Anti-Big-Tech activists rally around the slogan, “If you’re not paying for the product, you are the product.”<sup>1</sup> And because consumers are allegedly overpaying with their data, aggressive antitrust legislation and enforcement are justified so that big technology companies will have to compete on privacy.

While a creative device to justify breaking up Big Tech firms, this view is deeply flawed. First, unlike cash or physical goods, data is a nonrivalrous good; multiple people and organizations can access the same personal data at the same time, and the person is no worse off. Second, the “paying with data” view also rests on the false notion that consumers suffer when companies collect their data. In fact, virtually all targeted advertising by Big Tech firms is one-way blind: The tech companies’ computers have information on the customer, but the advertiser never does. This is why instances of consumers materially suffering from routine data collection on large platforms are extremely rare. Critics often label targeted ads based on consumer data as “creepy” and “invasive,” but they cannot point to concrete harms. Instead, they refer to abstract harms, such as arguing that ads facilitate political polarization, or point to harms about the substance of ads, such as those involving misinformation, hate speech, or targeting vulnerable groups.<sup>2</sup> Third, there is no evidence that most consumers choose platforms based on data-tracking practices. Therefore, more competition is unlikely to benefit consumer privacy.

Despite what detractors contend, collecting data for ad and service personalization creates valuable yet free online platforms for American consumers, allows businesses to efficiently and anonymously reach consumers, and creates high-paying jobs for American workers. To the extent policymakers are worried about online privacy, Congress should pass a national data privacy law that balances consumer concerns and the ability of firms to operate, including giving consumers the right to opt out of data collection, preempting state data privacy laws, and limiting private

right of action lawsuits. Using privacy concerns to justify aggressive antitrust action is misguided and the results would be harmful for consumers, especially low-income consumers who cannot afford monthly fees for now-free online services.

## **DATA IS NOT LIKE MONEY**

Despite allegations that “we pay for the service with our data,” as Sen. Mike Lee (R-UT) has claimed, comparisons between data and money don’t hold water.<sup>3</sup> Unlike money, data is nonrivalrous: Many different companies can collect, share, and use the same data simultaneously.<sup>4</sup> When consumers “pay with data” to access a website, they still have the same amount of data after the transaction as before. As a result, users have an infinite resource available to them to access free online services. In other words, if a customer pays \$5, they have \$5 less. But if an Internet user tells an online platform they are a soccer fan, both the user and the platform now have that information. Sharing data with one platform does not prevent a consumer from sharing that same data with another. Policymakers should therefore not treat data as if it is a limited resource that must be rationed.

Data tracking is not a new phenomenon. Across industries and even before the Internet age, businesses have been creating data about their customers. Credit card issuers itemize consumers’ purchases; telecom companies know what numbers their users call; loyalty-card issuers track purchases of their customers; electric utilities know how much electricity a household uses; schools know what students study and what their grades are; governments record what real estate people own, what countries they’ve visited, and so much more. No one doubts that these organizations own this data. Consumers might be able to see it, challenge its accuracy, or limit its use, but in no way does it belong to them—barring a few exceptions such as medical records.

Finally, while money is inherently valuable, ad-supported digital services turn data into value by connecting consumers and advertisers.<sup>5</sup> Users get access to a free service, and advertisers get access to an audience more likely to click on their ads. In almost all cases, the advertiser does not know which users see their ad, only that the ad is placed in front of a targeted group of people, such as people who live in Washington or have an interest in travel.<sup>6</sup>

---

**Policymakers should not treat data as if it is a limited resource that must be rationed.**

---

## **USE OF DATA TO TARGET ADS IS NOT A CONSUMER HARM**

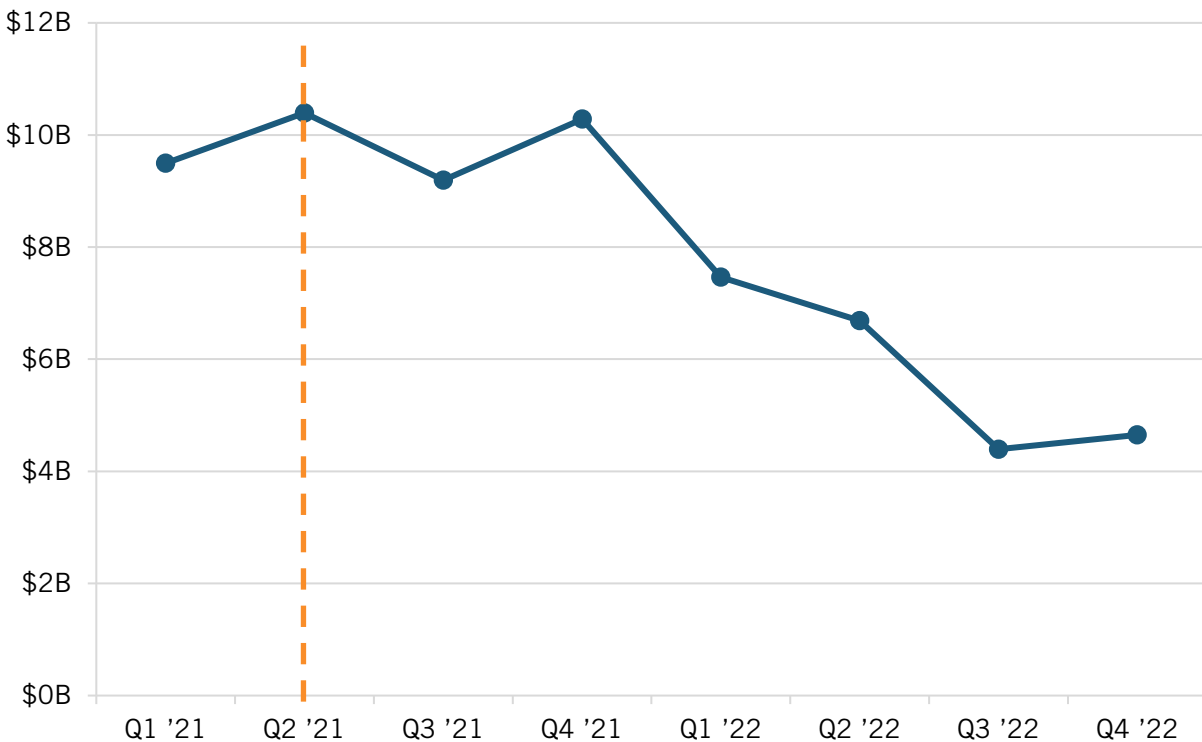
When people use online services such as Facebook and Google, machines—not humans—process user data. If a user sends a text to a friend talking about the party they went to last night, there is no person in a data center reading the text and noting it. Platforms use this data to run algorithms that provide their users with a customized experience: posts and advertisements that are more relevant to a user. Despite some people’s distrust, data tracking is, at the end of the day, making advertising more efficient for both advertisers and consumers. Targeted ads reduce irrelevant advertising, help customers discover new and useful products, make online search and shopping faster and easier, and boost revenues, including for small, ad-supported apps.

Instances of harm due to data collection by online platforms are uncommon; consumers can already take many steps to protect their information. For one, consumers can limit what information they provide to online services. In addition, many of the largest online platforms (e.g., Facebook, Instagram, and Snapchat) and search engines (e.g., Bing and Google) already offer consumers the ability to opt out of data collection, as well as provide consumers with various other privacy controls, so it is unclear what new privacy features more government-mandated competition would create.<sup>7</sup> And if a company’s privacy policy still does not satisfy consumers, they are free to not use the platform in favor of another one.

While the consumer costs of data tracking are limited, the costs of a too-restrictive privacy law would be massive. The main reason digital companies collect data is to better target ads because that generates more revenue, enabling them to invest more and improve service. A recent Information Technology and Innovation Foundation (ITIF) report finds that federal legislation mirroring key provisions of privacy laws in Europe or California would result in lower ad effectiveness costs of \$33 billion per year in the United States.<sup>8</sup> This would leave companies with far less to spend on designing new features for consumers.

A case in point, Apple’s App Tracking Transparency update, which required that users manually opt in to tracking on their devices, was predicted to decrease Facebook’s revenue by \$10 billion in 2022. Figure 1 shows that Facebook’s quarterly net income sank since Apple released the update in mid-2021. When companies cannot collect personal data, their ability to deliver targeted ads is compromised, stunting economic growth and user experience. Let’s be clear: This loss of Meta revenue is not a transfer payment in which consumers will gain back the value lost. It is a loss of economic efficiency for the whole economy.

**Figure 1: Meta quarterly net income, billions USD (2021–2022)<sup>9</sup>**

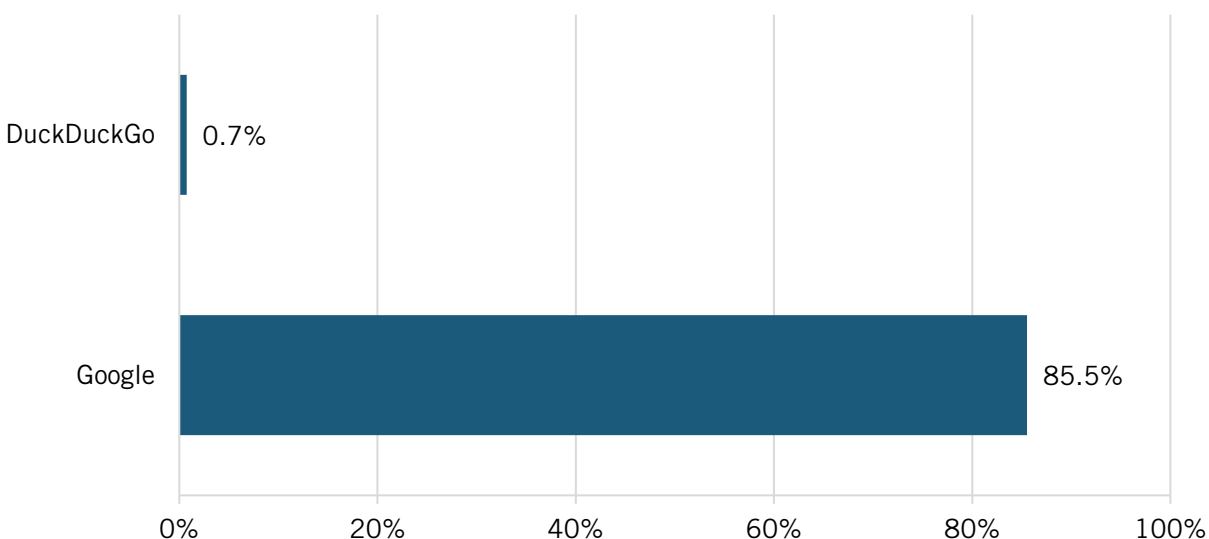


Start-ups also suffer from restrictive data-collection policies. The EU’s General Data Protection Regulation, which has made it much harder for companies to collect data from consumers, slashed start-up investment in the EU. A few weeks after the law was introduced, the average EU start-up earned 40 percent less than it did before the law came into force.<sup>10</sup>

## CONSUMERS ALREADY HAVE PRIVACY-PROTECTIVE OPTIONS

Alternatives that are nontargeted are available, but most consumers don’t seem to prefer them, so antitrust interventions are unlikely to change consumer privacy outcomes.<sup>11</sup> Several competitors to dominant platforms offer robust data protections. DuckDuckGo, for instance, is a search engine that neither tracks users nor collects or shares any personal information.<sup>12</sup> But even though DuckDuckGo was founded in 2008, its search engine market share (0.8 percent) still pales in comparison with Google’s over 85 percent market share (figure 2).<sup>13</sup> Internet users face nearly no switching costs when going from Google to DuckDuckGo. That Internet users aren’t switching to such an option suggests that they value the quality of the search service more than any alleged privacy benefit. Moreover, both Google and Bing allow users to search in private mode.<sup>14</sup>

**Figure 2: Search engine market shares: Google and DuckDuckGo (March 2023)<sup>15</sup>**



More competition will only improve privacy if consumers choose which platforms to use based on privacy protections. But there is no evidence that this is how consumers choose platforms; rather, DuckDuckGo’s trivial market share suggests that consumers attribute low importance to the privacy features of their online platforms. Further evidence confirms this; new entrant TikTok, for example, reached over 1 billion monthly active users despite using the same data collection practices as Facebook.<sup>16</sup>

The harder it is for companies to collect data, the harder it will be for them to personalize their services. And there is evidence that consumers want personalized online services. According to a report by McKinsey, 71 percent of consumers expect companies to deliver personalized interactions.<sup>17</sup> And 76 percent get frustrated when this doesn’t happen.<sup>18</sup> This may also play a role in why so-called “privacy protective” digital services have not taken off.

## **CONSUMERS DON'T WANT TO PAY FOR ONLINE SERVICES THAT ARE ALREADY FREE**

If policymakers expect the same quality of digital services platforms provide but don't allow them to earn more from targeted ads, the only answer will be to charge users subscription fees. But a shift toward subscription models would hurt many low- and middle-income individuals who would be forced to pay for online services that are currently free such as search engines, social networks, and mobile games.<sup>19</sup>

Moreover, most consumers would reject this option; people don't want companies to collect less data if that means paying for formerly free online services. According to a recent survey from ITIF's Center for Data Innovation, only one in four Americans want online services such as Facebook and Google to collect less of their data if it means they would have to start paying a monthly subscription fee.<sup>20</sup> American respondents were also far more willing to accept data tracking if it meant having a customized experience, more features, and free services.

## **CONCLUSION**

In their ongoing quest to transform the U.S. economy into a non-corporate one through aggressive antitrust enforcement, neo-Brandeisians seek any and all justifications for their radical objective. In the case of large technology platforms, a key justification is the canard that not only are “consumers paying with their data,” but that they are overpaying. Given that this is so far from users' experiences, it is amazing that it has gotten any traction whatsoever. But unfortunately, in a world of “techlash,” it has.

The reality is that Internet users are not paying for free services with their data the same way they might pay for online services with money. The exchange of data is a fundamentally different exchange of value than in other transactions. Data is nonrivalrous: When one business has access to it, it does not prevent others from using it. Moreover, advertising platforms do not share data with advertisers about which specific individuals have seen their ads. And so, while privacy violations that materially harm consumers are rare, the benefits of targeted advertising are large. Targeted advertising based on user data enables companies to provide extremely valuable services to consumers for free, supports a thriving R&D ecosystem, and creates a high-value-added tech sector that benefits American workers.

There is no evidence for the claim that using antitrust to create more competitors in select digital markets would somehow force companies to compete on privacy, and the scant market shares of existing privacy-focused options such as DuckDuckGo suggest that consumers don't choose platforms based on privacy. Breaking up Big Tech would imperil America's tech sector to the benefit of foreign rivals, especially large Chinese tech firms; nothing suggests it would boost privacy as some progressives claim.

To the extent that consumers are concerned about their online privacy, a federal data privacy law is the best way forward. Congress should act swiftly to pass comprehensive privacy legislation that preempts state laws, streamlines regulation, establishes basic consumer data rights, and minimizes the impact on innovation (e.g., by avoiding requirements for data minimization, universal opt-in, purpose specification, limitations on data retention, or privacy by design).<sup>21</sup> This would alleviate public concerns while protecting the digital industry and consumers from unwarranted breakups.

## Acknowledgments

The author would like to thank Rob Atkinson and Daniel Castro for their helpful contributions.

## About the Author

Hadi Houalla is a research assistant for antitrust policy at ITIF. He holds a B.A. in economics and statistics from the University of Virginia.

## About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit [itif.org/about](https://itif.org/about).

## ENDNOTES

---

1. Scott Goodson, "If You're Not Paying For It, You Become The Product," *Forbes*, March 5, 2012, <https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/?sh=77b121505d6e>; "If you're not paying, you are the product," Ted Talks (accessed August 21, 2023), [https://www.ted.com/talks/if\\_you\\_re\\_not\\_paying\\_you\\_are\\_the\\_product](https://www.ted.com/talks/if_you_re_not_paying_you_are_the_product).
2. Mozilla, "Report: The Dangers of AI-Powered Advertising (And How to Address Them)" (Mozilla, September 2019), <https://foundation.mozilla.org/en/blog/report-dangers-ai-powered-advertising-and-how-address-them/>.
3. Eileen McDermott, "Senators Tear into Facebook and Google Reps During 'Big Data, Big Questions' Hearing on Competition and Privacy," IPWatchdog, September 22, 2021, <https://ipwatchdog.com/2021/09/22/senators-tear-facebook-google-reps-big-data-big-questions-hearing-competition-privacy/id=137871/>. Ben Gilbert, "The #DeleteFacebook movement is a strong reminder that none of these 'free' services are truly free," *Insider*, March 26, 2018, <https://www.businessinsider.com/facebook-free-services-deletefacebook-2018-3?r=US&IR=T>.
4. "What Is a Rival Good vs. a Non-Rival Good, With Examples," Investopedia, accessed July 7, 2023, [https://www.investopedia.com/terms/r/rival\\_good.asp](https://www.investopedia.com/terms/r/rival_good.asp).
5. Andrei Hagiu and Julian Wright, "Multi-Sided Platforms," *International Journal of Industrial Organization*, Vol. 43 (March 2015), <http://dx.doi.org/10.2139/ssrn.2794582>.
6. Alan McQuinn, "No, Internet Users Are Not Paying With Their Data," Inside Sources, August 7, 2018, <https://insidesources.com/no-internet-users-not-paying-data/>.
7. "Meta Privacy Policy - How Meta collects and uses user data," Meta, accessed July 7, 2023, <https://www.facebook.com/privacy/policy/>; "Google Privacy Policy," Google, accessed July 7, 2023, <https://policies.google.com/privacy?hl=en-US>; Snapchat Privacy Policy," Snapchat, accessed July 7, 2023, <https://help.snapchat.com/hc/en-us/articles/7012345515796-How-to-Adjust-My-Advertising-Interest-Preferences-on-Snapchat>; "Microsoft Privacy Policy," Microsoft, accessed July 7, 2023, <https://privacy.microsoft.com/en-us/privacystatement>.
8. Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law" (ITIF, August 2019), <https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law/>.

9. “Net income generated by Meta from 1st quarter 2010 to 1st quarter 2023,” Statista, accessed July 7, 2023, <https://www.statista.com/statistics/223289/facebooks-quarterly-net-income/>.
10. Jian Jia et al., The Short-Run Effects of GDPR on Technology Venture Investment (working paper; November 2018), <https://www.nber.org/papers/w25248>; Mark Scott et al., “Six months in, Europe’s privacy revolution favors Google, Facebook,” *Politico*, November 23, 2018, <https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/>.
11. Ariel Ezrachi and Maurice Stucke, “The curious case of competition and quality,” *OUPblog*, July 21, 2015, <https://blog.oup.com/2015/07/competition-quality-law/>.
12. “DuckDuckGo Privacy Policy,” DuckDuckGo, accessed July 7, 2023, <https://duckduckgo.com/privacy>.
13. “Market share of leading desktop search engines worldwide from January 2015 to March 2023,” Statista, 2023, <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>.
14. “Google Privacy Policy,” Google, accessed July 7, 2023, <https://policies.google.com/privacy?hl=en-US>; “Microsoft Privacy Policy,” Microsoft, accessed July 7, 2023, <https://privacy.microsoft.com/en-us/privacystatement>.
15. “Market share of leading desktop search engines worldwide from January 2015 to March 2023,” Statista, 2023, <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>.
16. Amanda Silberling, “TikTok reached 1 billion monthly active users,” *TechCrunch*, September 27, 2021, <https://techcrunch.com/2021/09/27/tiktok-reached-1-billion-monthly-active-users/>.
17. Nidhi Arora et al., “The value of getting personalization right—or wrong—is multiplying,” McKinsey, November 12, 2021, <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying>
18. Ibid.
19. Daniel Castro and Alan McQuinn, “No, internet companies shouldn’t have to pay you for your data,” *The Sacramento Bee*, March 15, 2019, <https://www.sacbee.com/opinion/oped/article227760249.html>.
20. Daniel Castro and Michael McLaughlin, “Survey: Few Americans Willing to Pay for Privacy” (ITIF, January 2019), <https://datainnovation.org/2019/01/survey-few-americans-willing-to-pay-for-privacy/>.
21. Alan McQuinn and Daniel Castro, “A Grand Bargain on Data Privacy Legislation for America” (ITIF, January 2019), <https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america/>.